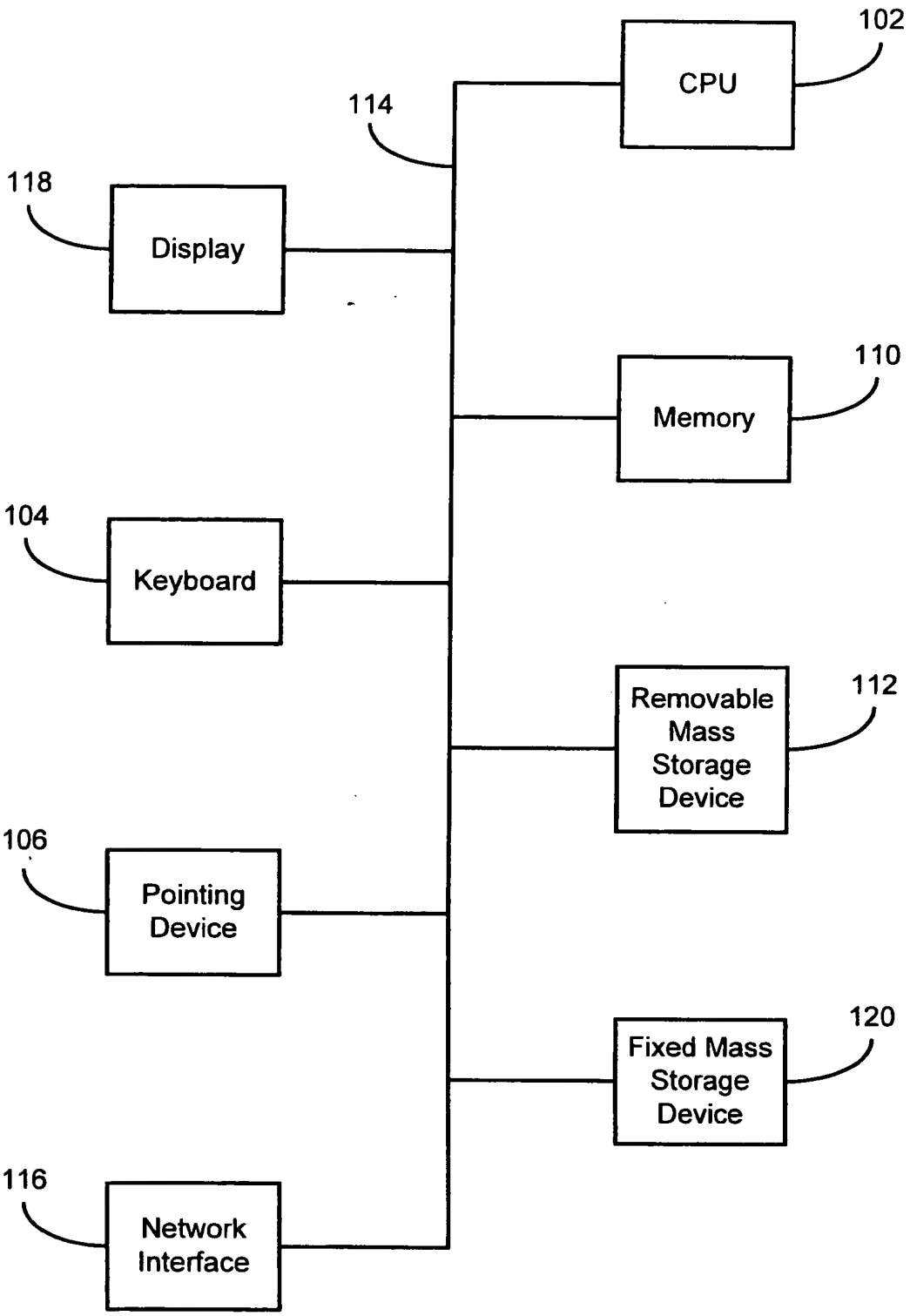
102
CPU
114
118
Display
110
Memory
104
Keyboard
112
Removable Mass Storage Device
106
Pointing Device
120
Fixed Mass Storage Device
116
Network Interface

FIG 1

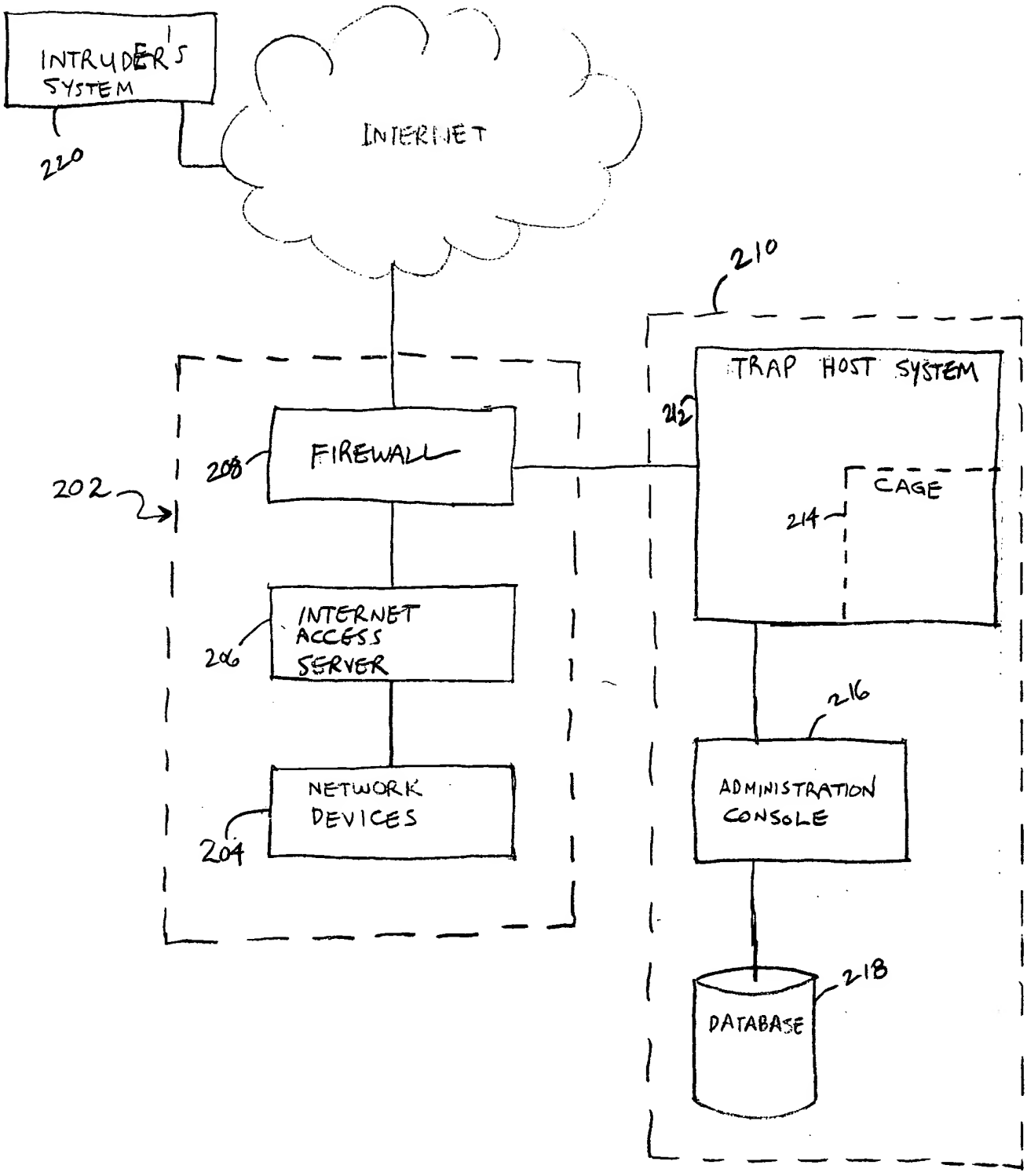
INTRUDER'S SYSTEM
220
INTERNET
210
TRAP HOST SYSTEM
212
FIREWALL
208
202
CAGE
214
INTERNET ACCESS SERVER
206
216
NETWORK DEVICES
204
ADMINISTRATION CONSOLE
DATABASE
218

FIG. 2

0004-2650-2650-0

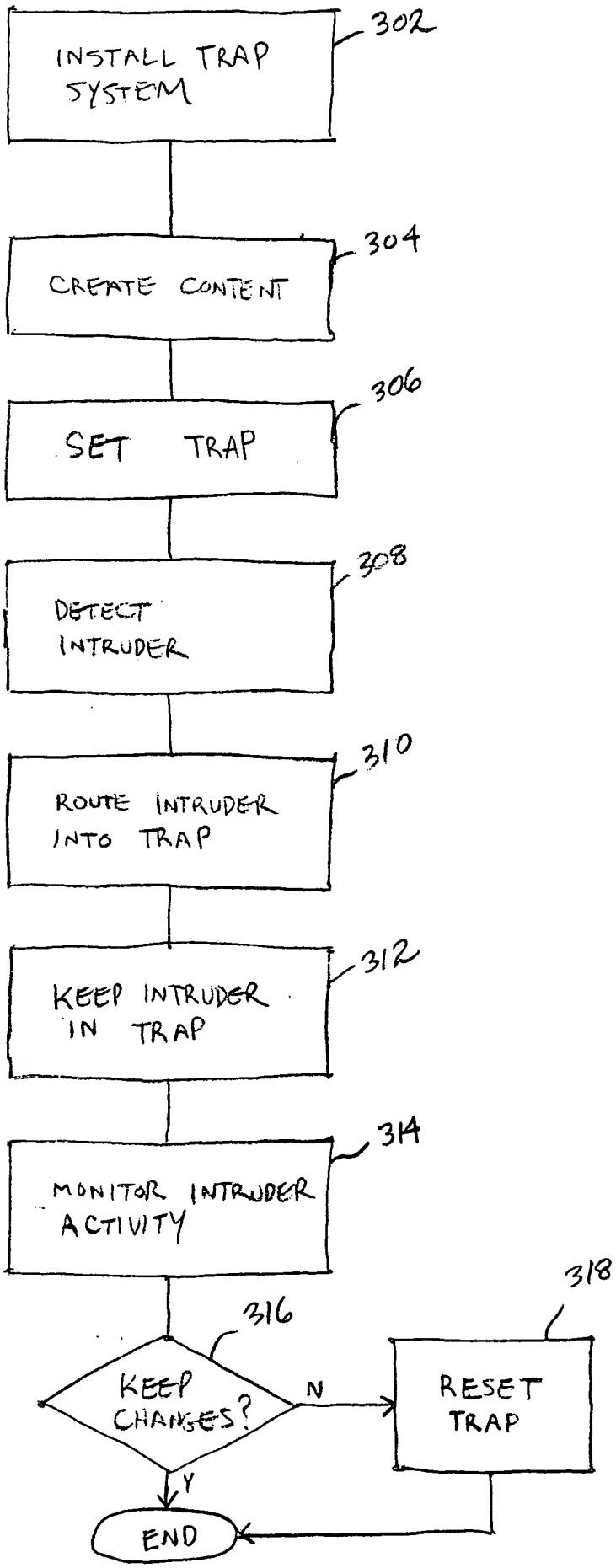

FIG. 3

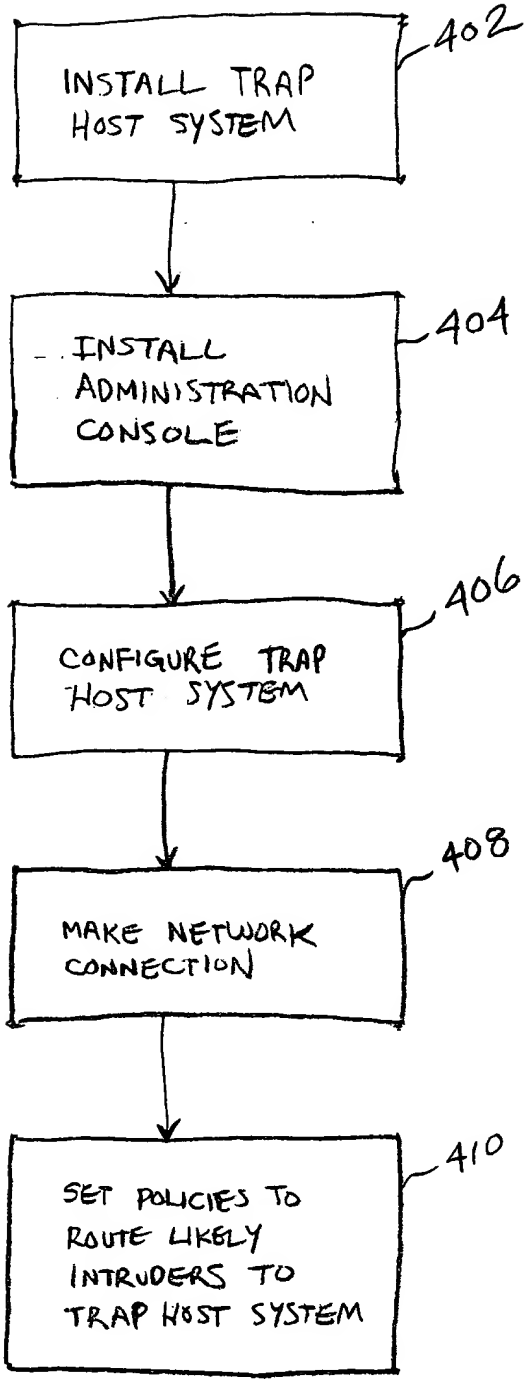
INSTALL TRAP HOST SYSTEM
402
INSTALL ADMINISTRATION CONSOLE
404
CONFIGURE TRAP HOST SYSTEM
406
MAKE NETWORK CONNECTION
408
SET POLICIES TO ROUTE LIKELY INTRUDERS TO TRAP HOST SYSTEM
410

FIG. 4

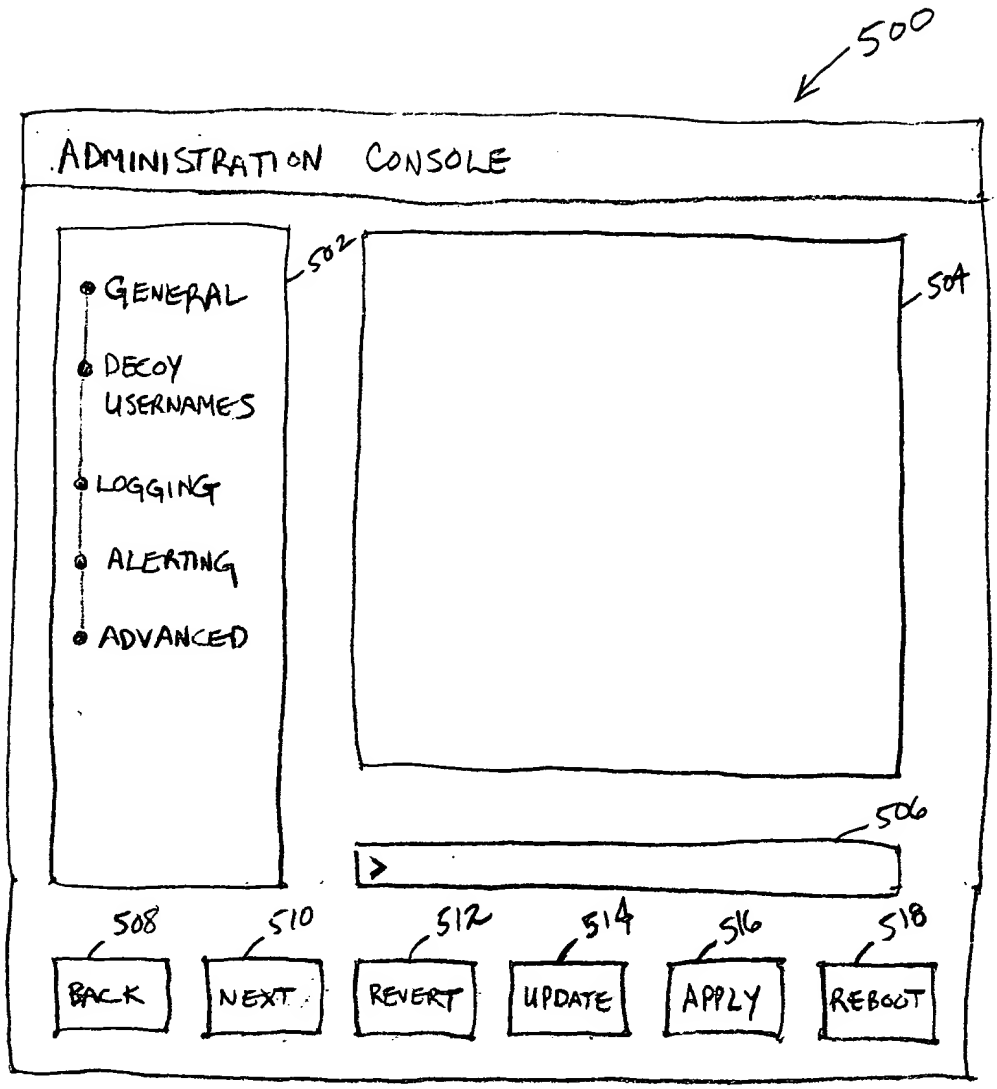
500
ADMINISTRATION CONSOLE
GENERAL
DECOY USERNAMES
LOGGING
ALERTING
ADVANCED
502
504
506
508
510
512
514
516
518
BACK
NEXT
REVERT
UPDATE
APPLY
REBOOT

FIG. 5

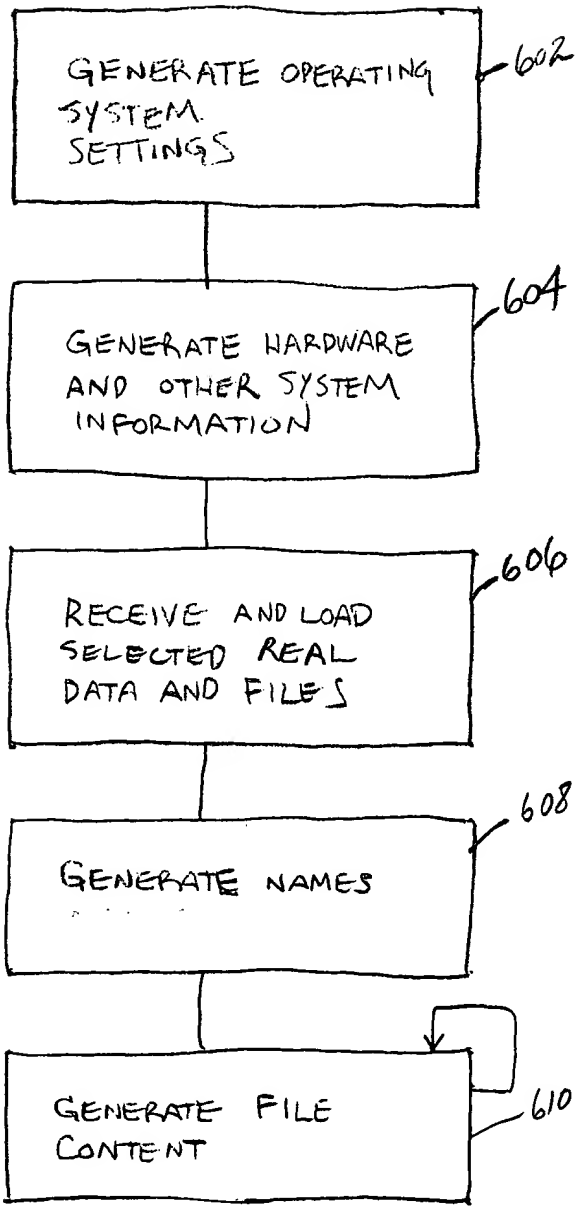
GENERATE OPERATING SYSTEM SETTINGS
602
GENERATE HARDWARE AND OTHER SYSTEM INFORMATION
604
RECEIVE AND LOAD SELECTED REAL DATA AND FILES
606
GENERATE NAMES
608
GENERATE FILE CONTENT
610

FIG. 6

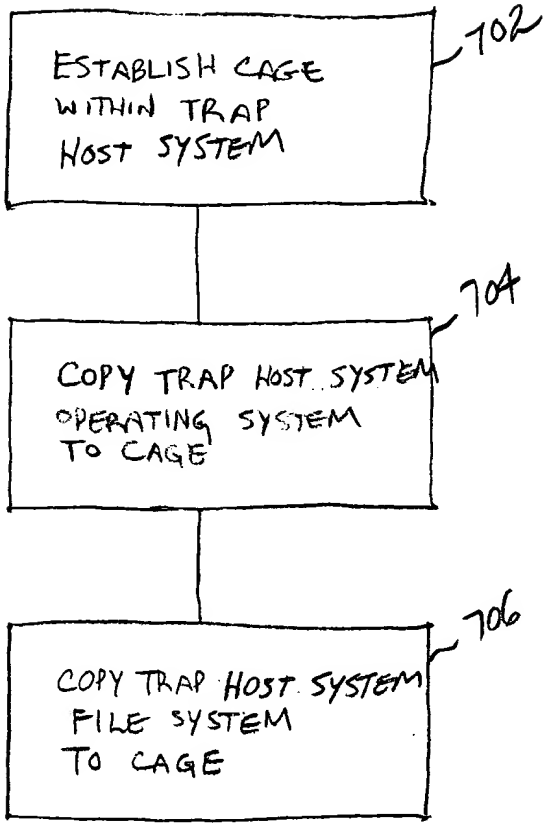
ESTABLISH CAGE WITHIN TRAP HOST SYSTEM
702
COPY TRAP HOST SYSTEM OPERATING SYSTEM TO CAGE
704
COPY TRAP HOST SYSTEM FILE SYSTEM TO CAGE
706

FIG. 7

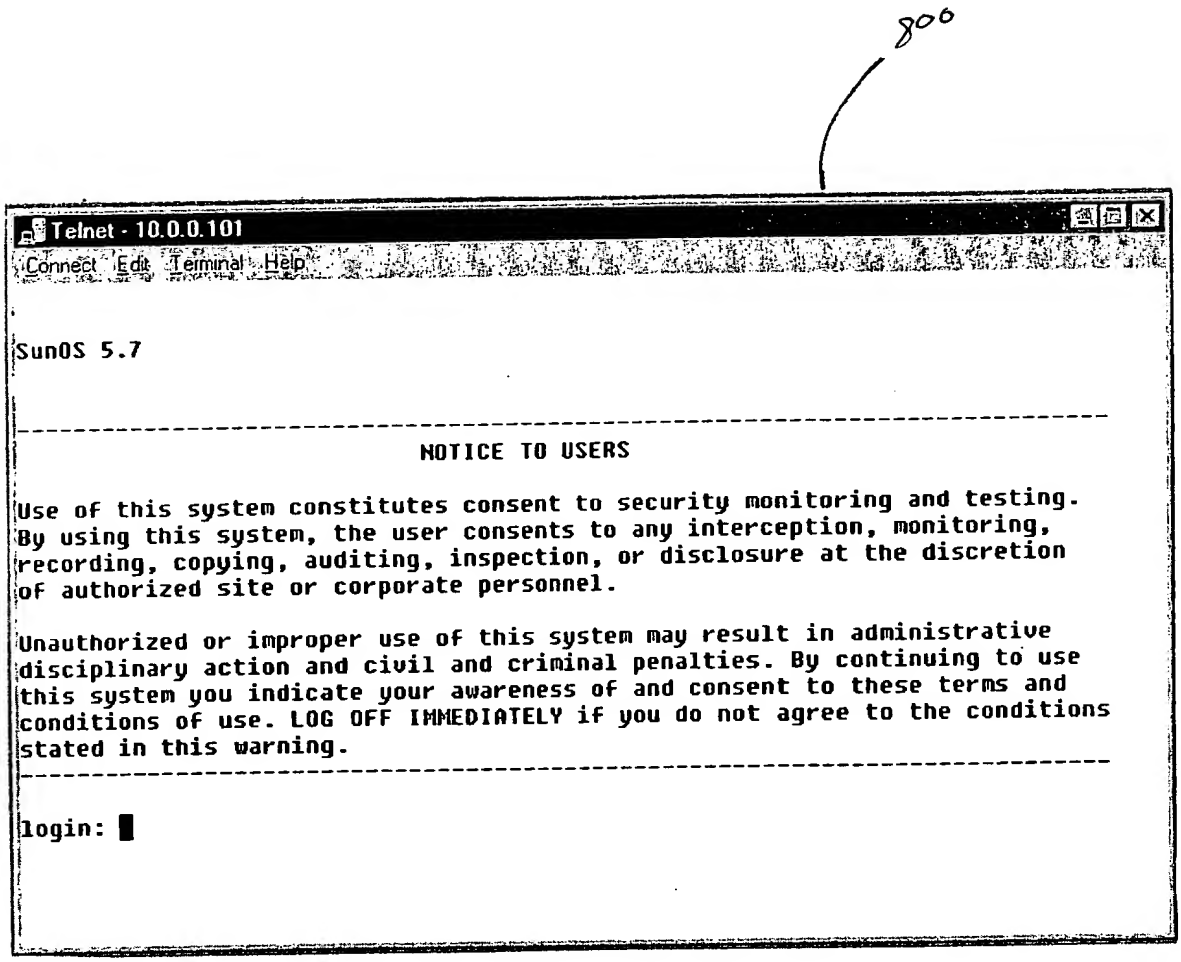
800
Telnet - 10.0.0.101
Connect Edit Terminal Help
SunOS 5.7
NOTICE TO USERS
Use of this system constitutes consent to security monitoring and testing. By using this system, the user consents to any interception, monitoring, recording, copying, auditing, inspection, or disclosure at the discretion of authorized site or corporate personnel.
Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.
login:

FIG. 8

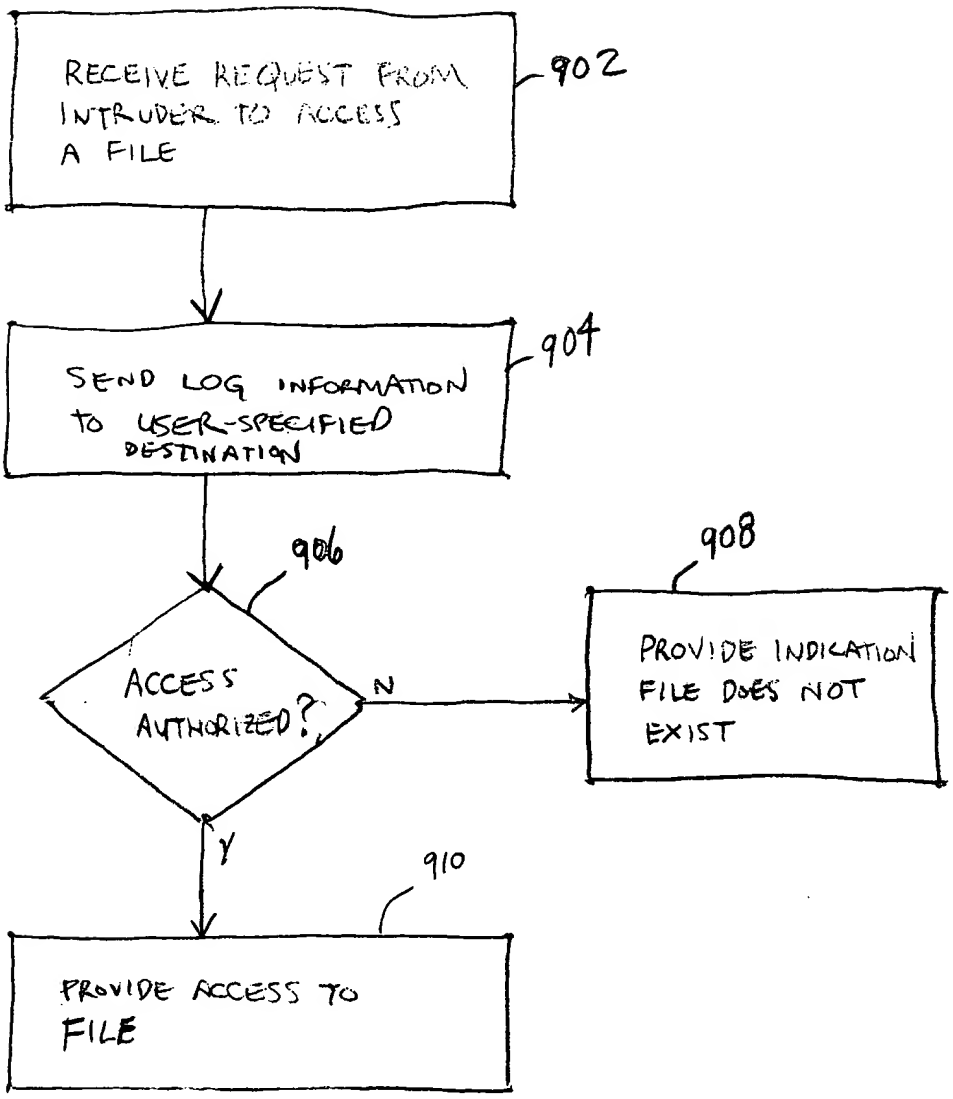
RECEIVE REQUEST FROM INTRUDER TO ACCESS A FILE
902
SEND LOG INFORMATION TO USER-SPECIFIED DESTINATION
904
906
ACCESS AUTHORIZED?
N
908
PROVIDE INDICATION FILE DOES NOT EXIST
Y
910
PROVIDE ACCESS TO FILE

FIG. 9

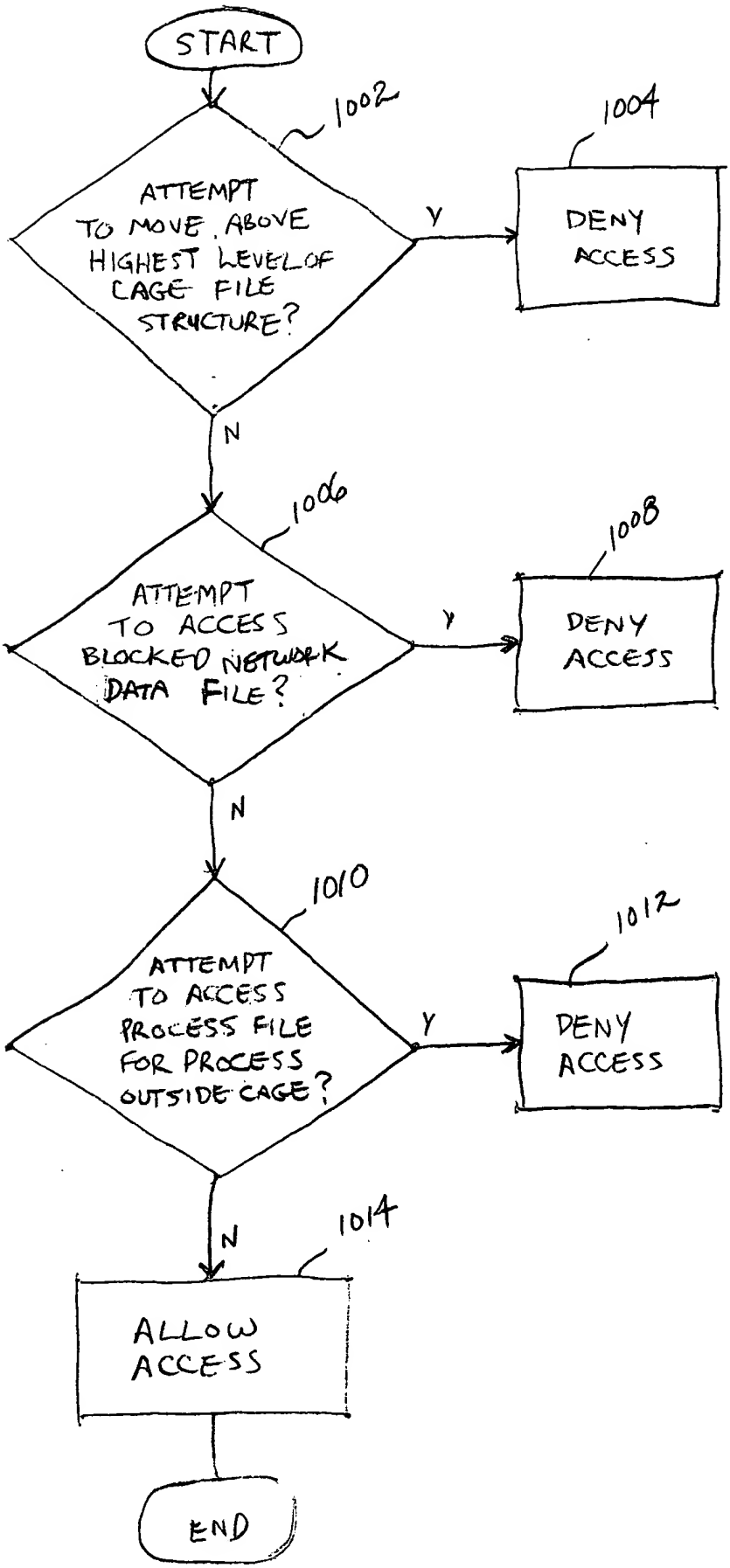
START
1002
ATTEMPT TO MOVE ABOVE HIGHEST LEVEL OF CAGE FILE STRUCTURE?
Y
1004
DENY ACCESS
N
1006
ATTEMPT TO ACCESS BLOCKED NETWORK DATA FILE?
Y
1008
DENY ACCESS
N
1010
ATTEMPT TO ACCESS PROCESS FILE FOR PROCESS OUTSIDE CAGE?
Y
1012
DENY ACCESS
N
1014
ALLOW ACCESS
END

FIG. 10

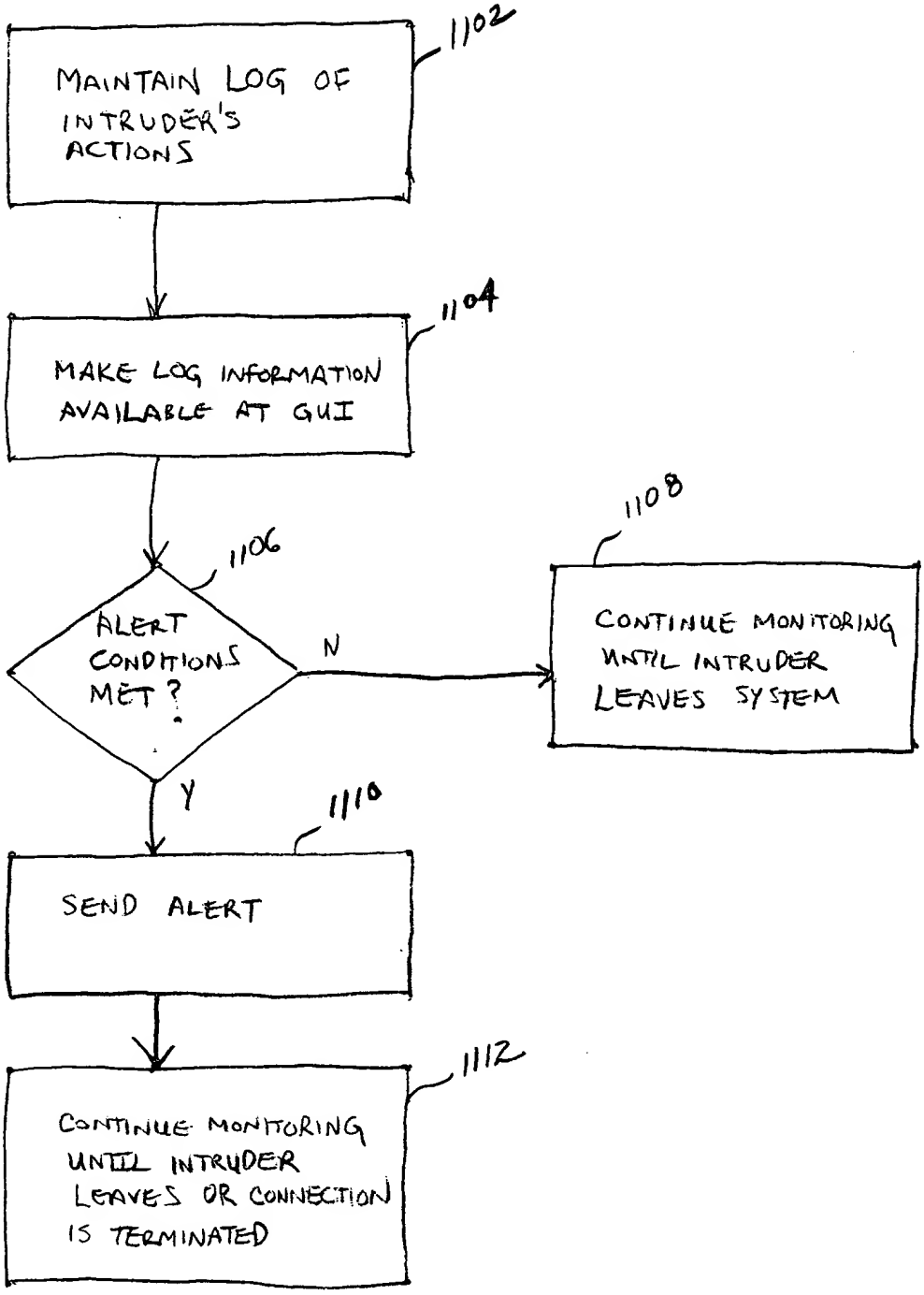
MAINTAIN LOG OF INTRUDER'S ACTIONS
1102
MAKE LOG INFORMATION AVAILABLE AT GUI
1104
ALERT CONDITIONS MET?
1106
N
CONTINUE MONITORING UNTIL INTRUDER LEAVES SYSTEM
1108
Y
SEND ALERT
1110
CONTINUE MONITORING UNTIL INTRUDER LEAVES OR CONNECTION IS TERMINATED
1112

FIG. 11A

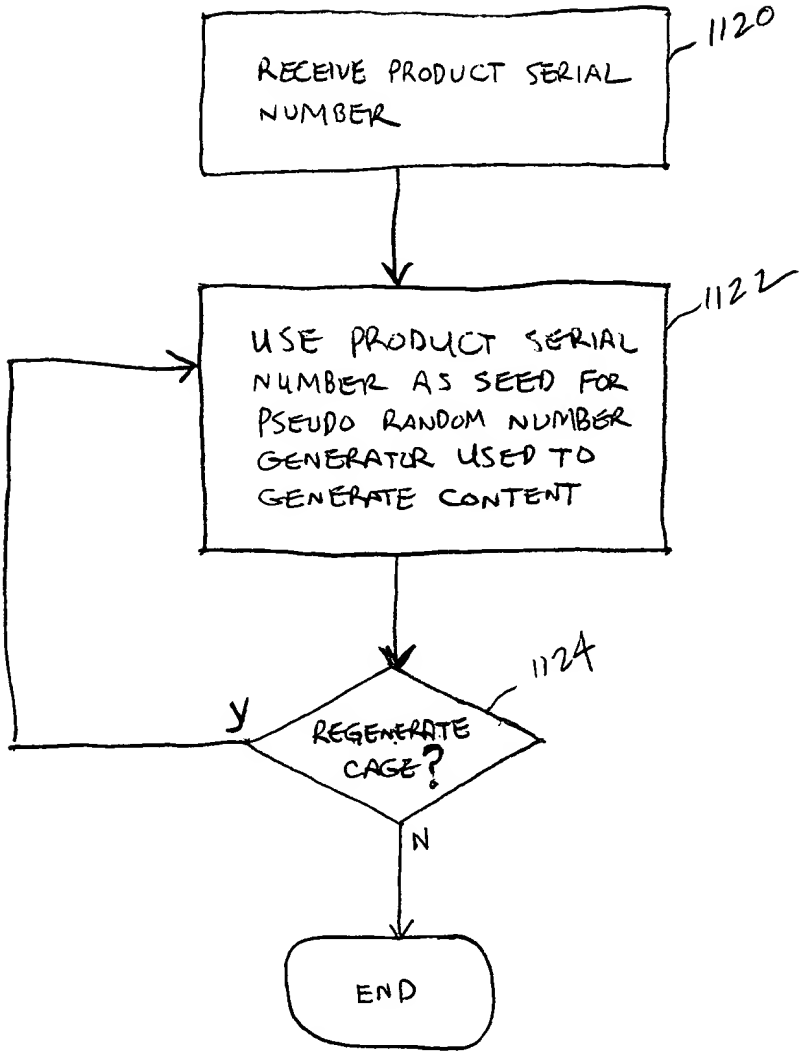
RECEIVE PRODUCT SERIAL NUMBER
1120
USE PRODUCT SERIAL NUMBER AS SEED FOR PSEUDO RANDOM NUMBER GENERATOR USED TO GENERATE CONTENT
1122
REGENERATE CAGE?
1124
Y
N
END

FIG. 11B

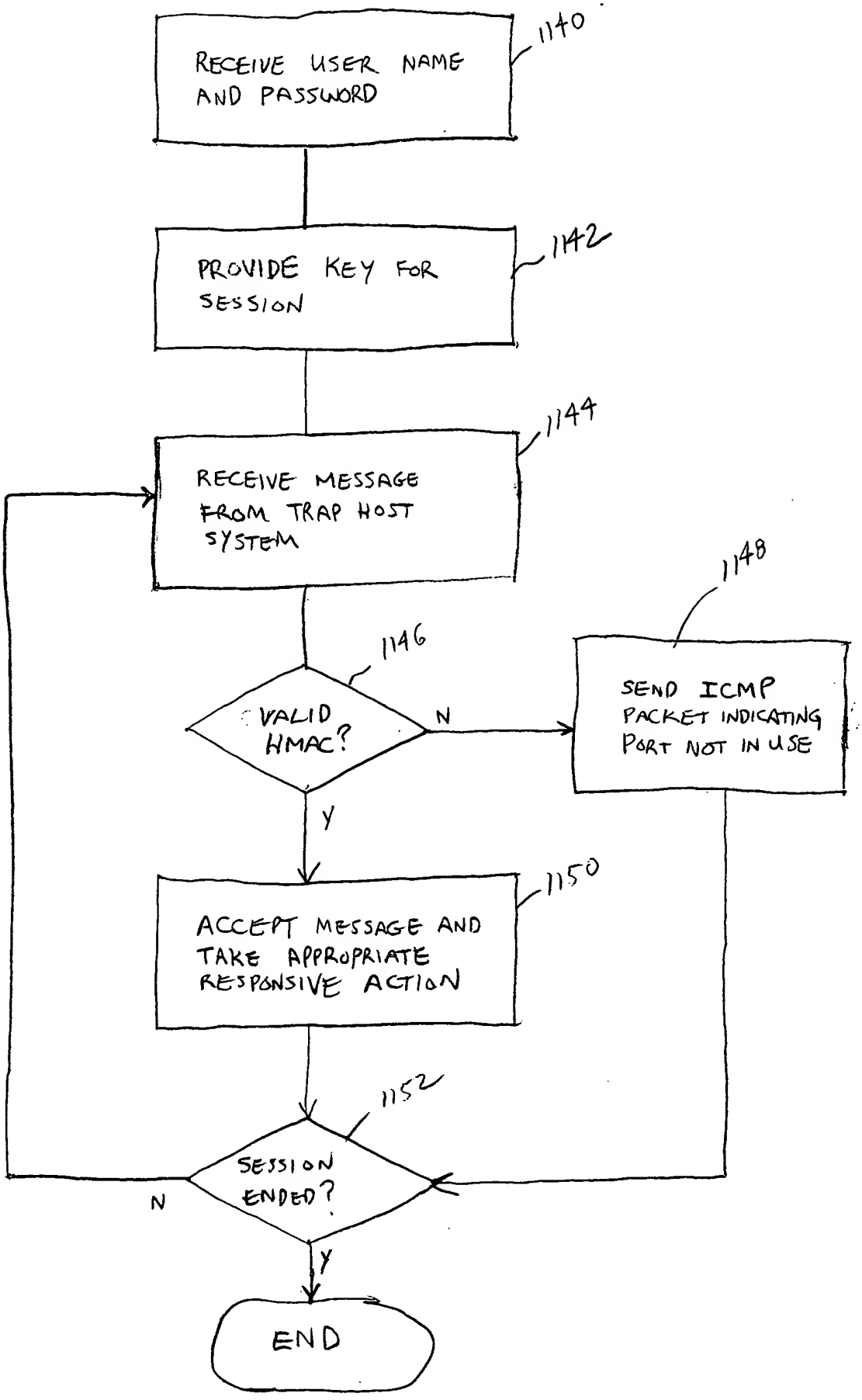
RECEIVE USER NAME AND PASSWORD
1140
PROVIDE KEY FOR SESSION
1142
RECEIVE MESSAGE FROM TRAP HOST SYSTEM
1144
VALID HMAC?
1146
N
SEND ICMP PACKET INDICATING PORT NOT IN USE
1148
Y
ACCEPT MESSAGE AND TAKE APPROPRIATE RESPONSIVE ACTION
1150
SESSION ENDED?
1152
N
Y
END

FIG. 11C

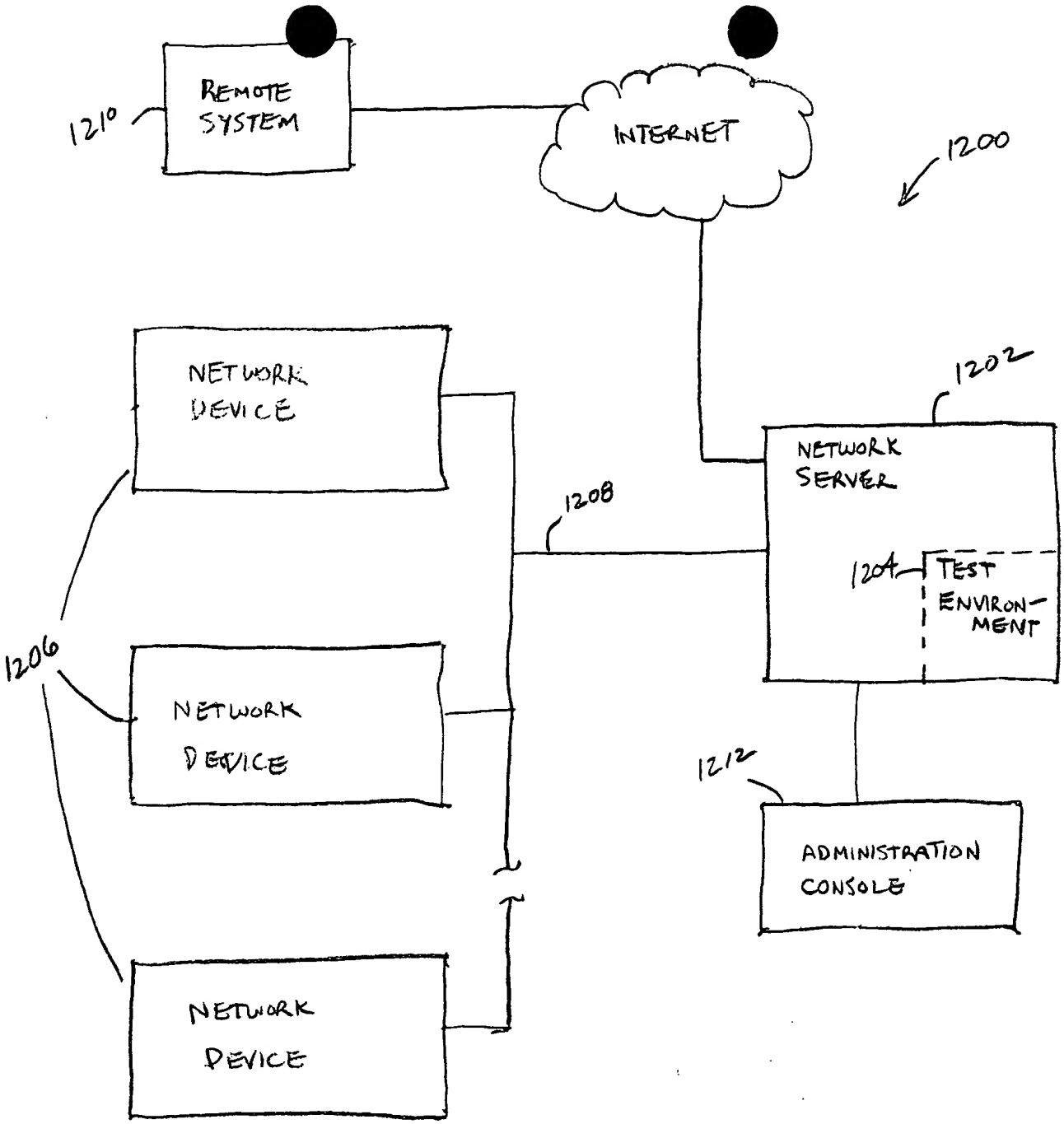
REMOTE SYSTEM
1210
INTERNET
1200
NETWORK DEVICE
NETWORK DEVICE
NETWORK DEVICE
1206
1208
1202
NETWORK SERVER
1204
TEST ENVIRON-MENT
1212
ADMINISTRATION CONSOLE

FIG. 12

DOCKET NO: 1565.1560

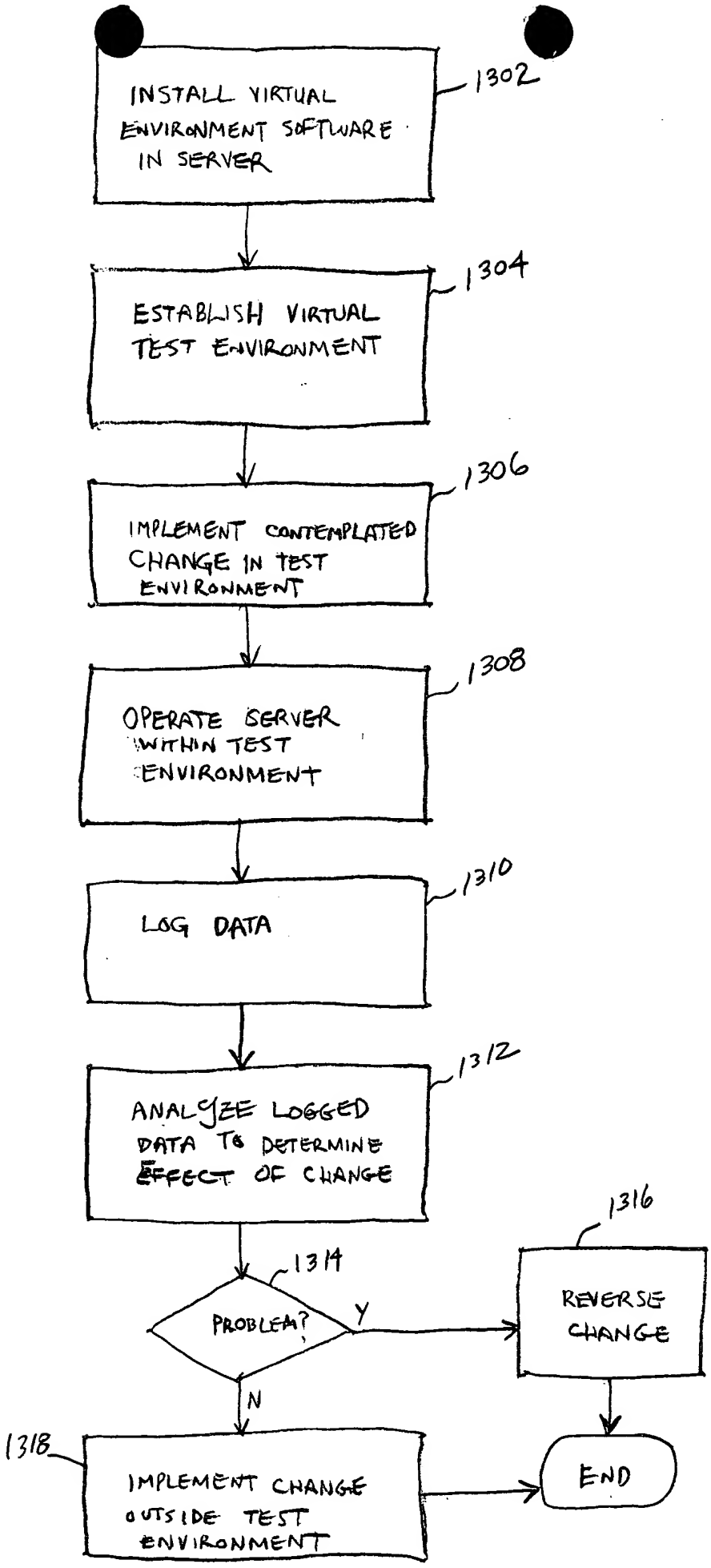

FIG. 13